Sentinel 7.3-Versionshinweise

Februar 2015

Sentinel 7.3 bietet neue Funktionen und ist einfacher in der Bedienung. Einige in früheren Versionen auftretende Probleme wurden behoben.

Viele der eingeführten Verbesserungen sind Umsetzungen von Vorschlägen unserer Kunden. Wir möchten uns auf diesem Wege bei Ihnen für Ihr wertvolles Feedback bedanken. Wir hoffen, Sie unterstützen uns weiterhin dabei, unsere Produkte optimal an Ihre Bedürfnisse anzupassen. Senden Sie uns Ihr Feedback als Beitrag im Sentinel-Forum in NetIQ Communities, unserer Online-Community. Hier finden Sie auch Produktinformationen, Blogs und Links zu weiteren nützlichen Ressourcen.

Die Dokumentation für dieses Produkt steht auf der NetIQ-Website im HTML- und PDF-Format zur Verfügung. Für den Zugriff auf diese Dokumentationsseite ist keine Anmeldung erforderlich. Wenn Sie uns einen Verbesserungsvorschlag in Bezug auf die Dokumentation mitteilen möchten, nutzen Sie die Schaltfläche **comment on this topic** (Kommentar zum Thema abgeben), die Sie unten auf jeder Seite der HTML-Version unserer auf der Sentinel NetIQ-Dokumentationswebseite veröffentlichten Dokumentation finden. Dieses Produkt steht auf der Website der Sentinel-Produktaufrüstung zum Herunterladen bereit.

- Abschnitt 1, „Neue Funktionen“, auf Seite 1
- Abschnitt 2, „Systemanforderungen“, auf Seite 9
- Abschnitt 3, „Installieren von Sentinel 7.3“, auf Seite 9
- Abschnitt 4, „Aufrüsten auf Sentinel 7.3“, auf Seite 9
- Abschnitt 5, „Bekannte Probleme“, auf Seite 9
- Abschnitt 6, „Kontaktangaben“, auf Seite 25
- Abschnitt 7, „Rechtliche Hinweise“, auf Seite 25

1 Neue Funktionen

In den folgenden Abschnitten werden wichtige Funktionen und Verbesserungen in dieser Version sowie die behobenen Probleme vorgestellt:

- Abschnitt 1.1, „Zentrale vereinheitlichte Plattform für Sentinel und Sentinel Log Manager“, auf Seite 2
- Abschnitt 1.2, „Warnmeldungsbenachrichtigungen und Selektierung“, auf Seite 2
- Abschnitt 1.3, „Warnmeldungs-Dashboards“, auf Seite 3
- Abschnitt 1.4, „Echtzeit-Ereignisansichten in der Weboberfläche“, auf Seite 3
- Abschnitt 1.5, „Plugin-Katalog“, auf Seite 3
- Abschnitt 1.6, „Appliance im OVF-Format“, auf Seite 3
- Abschnitt 1.7, „Verbesserungen der Konfiguration bei mehreren Mandanten“, auf Seite 3
- Abschnitt 1.8, „Verbesserungen bei korrelierten Ereignissen“, auf Seite 4
- Abschnitt 1.9, „Verbesserungen der Sicherheitsintelligenz-Dashboards“, auf Seite 4

- Abschnitt 1.10, „Terminologieänderungen für die Einrichtung mehrerer Instanzen (verteilte Einrichtung)“, auf Seite 5
- Abschnitt 1.11, „Verbesserungen der Sentinel-Lizenzierung“, auf Seite 5
- Abschnitt 1.12, „Ändern der Größe des Eigenschaftenfensters für dynamische Listen“, auf Seite 5
- Abschnitt 1.13, „Automatisches Löschen alter Berichte“, auf Seite 5
- Abschnitt 1.14, „Neueste Plugins“, auf Seite 5
- Abschnitt 1.15, „Softwarekorrekturen“, auf Seite 6

1.1 Zentrale vereinheitlichte Plattform für Sentinel und Sentinel Log Manager

NetIQ stellt Sentinel nun als zentrale Plattform für Sentinel- und Sentinel Log Manager-Lösungen bereit.

Die Sentinel-Plattform bietet zwei Hauptlösungen:

- **Sentinel Enterprise:** Eine umfassende Lösung, die neben der Echtzeit-Sicherheitsanalyse noch viele zusätzliche Funktionen bietet. Sentinel Enterprise ist auf SIEM-Anwendungsfälle ausgelegt, wie die Echtzeit-Bedrohungserkennung und Warnung und Abhilfe bei Bedrohungen.
- **Sentinel for Log Management:** Eine Lösung für die Protokollverwaltung, insbesondere zum Erfassen, Speichern und Durchsuchen der Daten und dem Erstellen von Berichten.

NetIQ bietet getrennte Lizenzen für diese beiden Lösungen. Bei der Erstinstallation werden je nach eingegebenem Lizenzschlüssel (Sentinel Enterprise oder Sentinel für Log Management) die entsprechenden Funktionen aktiviert. Vorhandene Sentinel-Server oder -Aufrüstungen sind nicht von dieser Änderung betroffen.

Weitere Informationen zu den Funktionen, die in den Lösungen jeweils aktiviert sind, finden Sie unter „Understanding License Information“ (Lizenzinformationen) im *NetIQ Installation and Configuration Guide* (NetIQ-Installations- und -Konfigurationshandbuch).

1.2 Warnmeldungsbenachrichtigungen und Selektierung

Korrelationsregeln können nun so konfiguriert werden, dass Sie bei einer möglichen Bedrohung eine sofortige Warnmeldungsbenachrichtigung erhalten. Warnmeldungen benachrichtigen Sie darüber, was Sie prioritär bearbeiten sollten. Warnmeldungen können sich auf Bedrohungen für IT-Ressourcen oder auf die Leistungsfähigkeit beziehen, etwa einen ausgelasteten Systemarbeitsspeicher oder nicht reagierende IT-Ressourcen. Sentinel verknüpft die relevanten Ereignisse und Identitäten automatisch mit den Warnmeldungen, damit Sie die Ursache der potenziellen Bedrohung einfacher ermitteln können.

Weitere Informationen finden Sie im Abschnitt „Configuring Alert Notifications“ (Konfigurieren der Warnmeldungsbenachrichtigungen) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Sentinel bietet eine grafische und eine tabellarische Darstellung der Warnmeldungen in den Echtzeit-Warnmeldungsansichten. Sie können Vorgänge zur Selektierung von Warnmeldungen ausführen, den Status einer Warnmeldung ändern, Warnmeldungen einem Benutzer oder einer Rolle zuweisen, Informationen zur Knowledge Base hinzufügen usw. Außerdem können Sie in jeder Warnmeldungsansicht Details anzeigen, wie das Auslöseereignis, die Identitäten der involvierten Benutzer und den Warnmeldungsverlauf. Weitere Informationen zur Warnmeldungsansicht finden Sie unter „Viewing and Triaging Alerts in Alert Views“ (Anzeigen und Selektieren von Warnmeldungen in der Warnmeldungsansicht im „*NetIQ Sentinel User Guide*“ (NetIQ Sentinel-Benutzerhandbuch).

1.3 Warnmeldungs-Dashboards

Die Warnmeldungs-Dashboards sind ein leistungsfähiges Tool zur Auswertung und Analyse der Warnmeldungen. Das Warnmeldungs-Dashboard stellt eine einfach zu konfigurierende, anpassbare Benutzeroberfläche dar, mit der Sie Warnmeldungen detailliert anzeigen und untersuchen können. Hier können Sie beispielsweise ermitteln, wie lange die Eigentümer durchschnittlich zum Schließen einer Warnmeldung benötigen oder welche Korrelationsregel die meisten Warnmeldungen generiert, oder die durchschnittliche Anzahl an konsolidierten Warnmeldungen oder den geografischen Standort der Warnmeldungen mit hohem Schweregrad anzeigen. Weitere Informationen zu Warnmeldungs-Dashboards finden Sie unter „Analyzing Alert Dashboards“ (Warnmeldungs-Dashboards analysieren) im „*NetIQ Sentinel User Guide*“ (NetIQ Sentinel-Benutzerhandbuch).

1.4 Echtzeit-Ereignisansichten in der Weboberfläche

Sie können Ereignisse nun in Echtzeit in der Sentinel-Weboberfläche anzeigen, ohne sich am Sentinel Control Center anmelden zu müssen. Echtzeit-Ereignisansichten bieten eine zusammenfassende Übersicht der Ereignisdaten. Verwenden Sie die Suchoberfläche, wenn Sie Details zu einem Ereignis anzeigen oder Ereignisvorgänge ausführen möchten. Weitere Informationen zum Anzeigen von Echtzeit-Ereignisansichten in der Weboberfläche finden Sie unter „Viewing Events in the Web Interface“ (Ereignisse in der Weboberfläche anzeigen) im *NetIQ Sentinel User Guide* (NetIQ Sentinel-Benutzerhandbuch).

1.5 Plugin-Katalog

Sie können nun eine Liste der auf dem Sentinel-Server installierten Plugins anzeigen. Die Oberfläche **Plugins** > **Katalog** führt alle Collectors, Connectors, Aktionen, Integratoren und Feeds auf, die auf dem Sentinel-Server installiert sind. Außerdem können Sie die Version, das Veröffentlichungsdatum und andere Metadaten der Plugins anzeigen, um einfacher ermitteln zu können, ob die jeweils neueste Version eines Plugins installiert ist. Zum Anzeigen der Plugin-Liste müssen Sie über die Administratorrolle verfügen.

1.6 Appliance im OVF-Format

Sentinel bietet die Appliance nun im Open Virtual Machine(OVF)-Format an. Dies bietet den Vorteil, dass nicht mehr verschiedene Appliance-Formate für die einzelnen Virtualisierungssoftwares benötigt werden. Die Sentinel-OVF-Appliance ersetzt die VMware- und Xen-Appliances. Sie können Sentinel mit der OVF-Appliance auf VMware- oder auf Citrix Xen-Virtualisierungsplattformen installieren. Die Appliance-Aktualisierungen im NCC-Kanal aktualisieren weiterhin die vorhandenen Appliances im Xen- oder VMware-Format. Weitere Informationen zur Installation der Sentinel-Appliance im OVF-Format finden Sie unter „Installing OVF Appliance“ (OVF-Appliance installieren) im *NetIQ Sentinel Installation and Configuration Guide* (NetIQ Sentinel-Installations- und -Konfigurationshandbuch).

1.7 Verbesserungen der Konfiguration bei mehreren Mandanten

Sentinel 7.3 bietet mehrere Verbesserungen zur Unterstützung von Konfigurationen mit mehreren Mandanten für MSSPs (Managed Security Services Provider):

- **Möglichkeit zur Verwaltung von Mandanten:** Eine neue Benutzeroberfläche bietet Ihnen die Möglichkeit, Mandanten vorab zu erstellen, bevor Daten vom Mandanten empfangen werden. Über diese Benutzeroberfläche können Sie die Mandanten außerdem aktivieren und deaktivieren.

- **Mandantenspezifische Rollen und Benutzer:** Beim Erstellen einer Rolle können Sie nun dem standardmäßigen Mandanten oder einem bestimmten Mandanten eine Rolle zuweisen. Der standardmäßige Mandant bietet Zugriff auf die Daten aller Mandanten. Sie können den standardmäßigen Mandanten in Umgebungen ohne Mandant und für MSSP-Benutzer verwenden, die Zugriff auf die Daten aller Mandanten benötigen. Benutzer in einer Rolle, die einem bestimmten Mandanten zugewiesen ist, können nur die Daten anzeigen, die mit dem Namen dieses Mandanten gekennzeichnet sind. MSSP-Mitarbeiter, die Daten mehrerer Mandanten anzeigen können müssen, können dem standardmäßigen Mandanten zugewiesen werden. So haben sie Zugriff auf die Daten und Echtzeit-Ansichten aller Mandanten.

Ausführliche Informationen zu diesen Verbesserungen und zur Konfiguration mit mehreren Mandanten finden Sie unter „Configuring Sentinel in Multi-Tenancy Environments“ (Sentinel im Umgebungen mit mehreren Mandanten konfigurieren) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

1.8 Verbesserungen bei korrelierten Ereignissen

Sentinel 7.3 bietet folgende Verbesserungen in Bezug auf korrelierte Ereignisse:

- **Anpassen des korrelierten Ereignisses:** In der Benutzeroberfläche für die **Korrelation** ist nun eine Option enthalten, mit der Sie die Feldwerte der korrelierten Ereignisse beim Erstellen der Korrelationsregel anpassen können. Wenn ein korreliertes Ereignis beispielsweise einen anderen Schweregrad aufweisen soll als seine Auslöseereignisse, können Sie einen neuen Wert für den Schweregrad festlegen. Weitere Informationen finden Sie unter „Customizing Correlated Event“ (Korreliertes Ereignis anpassen) im *NetIQ Sentinel User Guide* (NetIQ Sentinel-Benutzerhandbuch).
- **Konfigurieren der Anzahl der Auslöseereignisse:** Sie können nun die Anzahl der Auslöseereignisse festlegen, die mit einer Korrelationsregel verknüpft werden können. Durch das Festlegen einer Obergrenze wird verhindert, dass Sentinel eine hohe Anzahl Auslöseereignisse mit dem korrelierten Ereignis verknüpft. Dies reduziert die Last auf dem Server. Weitere Informationen finden Sie unter „Configuring the Number of Trigger Events to Associate with a Correlated Event“ (Konfigurieren der Anzahl der Auslöseereignisse, die mit einem korrelierten Ereignis verknüpft werden können) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

1.9 Verbesserungen der Sicherheitsintelligenz-Dashboards

Sentinel 7.3 bietet folgende Verbesserungen der Sicherheitsintelligenz-Dashboards:

- **Einschließen von Verlaufsdaten:** Beim Auffüllen der Sicherheitsintelligenzdaten im Dashboard können Sie nun Verlaufsdaten einschließen. Dies bietet zusätzlichen Kontext für das Analysieren der Daten.
- **Größere Datenbeibehaltungszeiträume:** Sie können die Sicherheitsintelligenzdaten nun bis zu 64 Wochen beibehalten.

Weitere Informationen finden Sie im Abschnitt „Creating a Dashboard“ (Erstellen eines Dashboards) im *NetIQ Sentinel User Guide* (NetIQ Sentinel-Benutzerhandbuch).

1.10 Terminologieänderungen für die Einrichtung mehrerer Instanzen (verteilte Einrichtung)

Sentinel 7.3 verwendet neue Terminologie in der Benutzeroberfläche für die Einrichtung mehrerer Instanzen (verteilte Einrichtung). Diese Änderungen spiegeln wider, dass die Einrichtung mehrerer Instanzen für Datenverbunde ausgelegt und nicht spezifisch für Suchen oder Ereignisse ist. Folgende Terminologieänderungen wurden eingeführt:

- „Verteilte Suche“ ist jetzt „Datenverbund“
- „Ziele“ ist jetzt „Datenquellen“
- „Suchzielserver“ ist jetzt „Datenquellenserver“
- „Suchinitiatorserver“ ist jetzt „Autorisierter Requester“

Weitere Informationen finden Sie unter „Configuring Data Federation“ (Datenverbund konfigurieren) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

1.11 Verbesserungen der Sentinel-Lizenzierung

Mit der standardmäßigen Probelizenz einer Erstinstallation von Sentinel können Sie alle Funktionen von Sentinel Enterprise im Probezeitraum von 60 Tagen mit unbegrenzter EPS nutzen. Nach dem Ablauf der Probelizenz wird das System mit einer kostenlosen Lizenz ausgeführt, die eine Verwendung mit eingeschränktem Funktionsumfang und begrenzter Ereignisrate von 25 EPS zulässt. Die kostenlose Lizenz läuft nie ab. Weitere Informationen zu Sentinel-Lizenzen finden Sie unter „Understanding License Information“ (Lizenzinformationen) im *NetIQ Installation and Configuration Guide* (NetIQ-Installations- und -Konfigurationshandbuch).

1.12 Ändern der Größe des Eigenschaftenfensters für dynamische Listen

Sie können nun die Größe des Eigenschaftenfensters für dynamische Listen ändern, sodass lange Werte einfacher angezeigt werden können.

1.13 Automatisches Löschen alter Berichte

Sentinel löscht automatisch alte Berichte, um die Speicherplatzauslastung zu optimieren. Sie können den Beibehaltungszeitraum für die Berichte beliebig definieren. Weitere Informationen finden Sie im Abschnitt „Configuring the Report Retention Period“ (Beibehaltungszeitraum für Berichte konfigurieren) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

1.14 Neueste Plugins

Sentinel 7.3 umfasst neue und aktualisierte Versionen der Sentinel-Plugins. Die aktuelle Version der Collectors und Connectors ist erst nach einer Neuinstallation verfügbar. Die aktuelle Version der Integratoren und Aktionen ist sowohl nach einer Neuinstallation als auch nach einer Aufrüstung verfügbar. Bei einer Aufrüstung auf Sentinel 7.3 informieren Sie sich zunächst auf der Website der Sentinel-Plugins über den Versionsverlauf der aktuellen Collectors und Connectors in der zugehörigen Dokumentation, und entscheiden Sie dann, welche Plugins heruntergeladen und installiert werden sollen.

1.15 Softwarekorrekturen

Sentinel 7.3 enthält einige Softwarekorrekturen zur Behebung mehrerer Probleme.

Eine Liste der Softwarekorrekturen und Erweiterungen in früheren Versionen finden Sie in den entsprechenden Versionshinweisen.

- Abschnitt 1.15.1, „Ergebnisse einer verteilten Suche mit mehr als 50.000 Ereignissen können nicht exportiert werden“, auf Seite 6
- Abschnitt 1.15.2, „Rohdatenpuffer hat für das Speichern eingehender Daten eine festgelegte Größenbeschränkung“, auf Seite 6
- Abschnitt 1.15.3, „Korrelationsregel kann nicht neu bereitgestellt werden, wenn mehrere Regelregisterkarten geöffnet sind“, auf Seite 7
- Abschnitt 1.15.4, „Eingabetaste muss bei einer Ereignissuche zweimal gedrückt werden“, auf Seite 7
- Abschnitt 1.15.5, „Change Guardian-Ereignisdetails können ohne Change Guardian-Lizenzschlüssel nicht angezeigt werden“, auf Seite 7
- Abschnitt 1.15.6, „Installationsprogramm für Appliance-Aufrüstung löscht während der Aufrüstung benutzerdefinierte Firewall-Regeln“, auf Seite 7
- Abschnitt 1.15.7, „Fehler beim Verarbeiten von Rohdaten“, auf Seite 7
- Abschnitt 1.15.8, „Attributfilter in der Ereignisquellenansicht erweitert die Ereignisquellen nicht automatisch“, auf Seite 7
- Abschnitt 1.15.9, „Sentinel zeigt die Change Guardian-Ereignisanlagen nach einem Anzeigen nicht mehr an“, auf Seite 8
- Abschnitt 1.15.10, „Unzuverlässige Datenbanksynchronisierung zwischen Sentinel und Sentinel Agent Manager“, auf Seite 8
- Abschnitt 1.15.11, „Ereignisfelder in Bezug auf den geografischen Standort werden nicht mit den richtigen Daten aufgefüllt“, auf Seite 8
- Abschnitt 1.15.12, „Skript „clean_db.sh“ löscht die Advisor-Daten in benutzerdefinierten Installationen nicht“, auf Seite 8
- Abschnitt 1.15.13, „Verbindungsprobleme zwischen Clients und Sentinel im FIPS-Modus“, auf Seite 8
- Abschnitt 1.15.14, „Ereignissuche funktioniert nicht nach einer fehlgeschlagenen verteilten Suche“, auf Seite 9

1.15.1 Ergebnisse einer verteilten Suche mit mehr als 50.000 Ereignissen können nicht exportiert werden

Problem: Es ist nicht möglich, verteilte Suchergebnisse mit mehr als 50.000 Ereignissen in eine Datei zu exportieren. (`BUG 863985`)

Korrektur: Sie können nun Suchergebnisdateien mit bis zu 200.000 Ereignissen exportieren.

1.15.2 Rohdatenpuffer hat für das Speichern eingehender Daten eine festgelegte Größenbeschränkung

Problem: Der Rohdatenpuffer hat für das Speichern eingehender Daten eine festgelegte Größenbeschränkung. Wenn die eingehenden Daten die Grenze überschreiten, verwirft Sentinel die Rohdaten, auch wenn ausreichend Speicherplatz vorhanden ist. (`BUG 893546`)

Korrektur: Die Größe des Rohdatenpuffers ist nicht eingeschränkt. Sentinel kann Rohdaten im Puffer speichern, bis der Speicherplatz zu 90 % ausgelastet ist.

1.15.3 Korrelationsregel kann nicht neu bereitgestellt werden, wenn mehrere Regelregisterkarten geöffnet sind

Problem: Korrelationsregeln können nicht bereitgestellt werden, wenn gleichzeitig mehrere Regelregisterkarten geöffnet sind. (BUG 838771)

Korrektur: Sie können Korrelationsregeln nun neu bereitstellen, wenn mehrere Regelregisterkarten gleichzeitig geöffnet sind.

1.15.4 Eingabetaste muss bei einer Ereignissuche zweimal gedrückt werden

Problem: Wenn Sie eine Ereignissuche ausführen und die Suchabfrage bearbeiten, müssen Sie zweimal die Eingabetaste drücken oder zweimal auf **Suche** klicken, bevor die Suche gestartet wird.(BUG 829291)

Korrektur: Die Ereignissuche beginnt, wenn Sie nach dem Bearbeiten einer Suchabfrage einmal die Eingabetaste drücken oder auf **Suche** klicken.

1.15.5 Change Guardian-Ereignisdetails können ohne Change Guardian-Lizenzschlüssel nicht angezeigt werden

Problem: Wenn Sie zum Anzeigen von Ereignisdetails auf das Symbol „Change Guardian“ klicken, fordert Sentinel Sie zur Eingabe der Change Guardian-Lizenz auf. (BUG 855914)

Korrektur: Sie können nun die Change Guardian-Details anzeigen, ohne den Change Guardian-Lizenzschlüssel eingeben zu müssen.

1.15.6 Installationsprogramm für Appliance-Aufrüstung löscht während der Aufrüstung benutzerdefinierte Firewall-Regeln

Problem: Während der Aufrüstung einer Sentinel-Appliance löscht Sentinel vorhandene benutzerdefinierte Firewall-Regeln. (BUG 867662)

Korrektur: Sentinel 7.3 behält die vorhandenen benutzerdefinierten Firewall-Regeln bei.

1.15.7 Fehler beim Verarbeiten von Rohdaten

Problem: Rohdatendateien, die nicht richtig geschlossen wurden, werden von Sentinel nicht verarbeitet. Dieses Problem tritt nur sporadisch auf. (BUG 870969)

Korrektur: Sentinel 7.3 verarbeitet nun auch Rohdatendateien, die nicht richtig geschlossen wurden.

1.15.8 Attributfilter in der Ereignisquellenansicht erweitert die Ereignisquellen nicht automatisch

Problem: In der Tabellenansicht der Ereignisquellenverwaltung wird beim Filtern der Attribute eine reduzierte Ansicht der Ereignisquellen angezeigt. Sie müssen die Ansicht manuell erweitern. (BUG 790041)

Korrektur: In Sentinel 7.3 wird die Ansicht der Ereignisquellenverwaltung automatisch erweitert, wenn Sie nach Attributen filtern.

1.15.9 Sentinel zeigt die Change Guardian-Ereignisanlagen nach einem Anzeigen nicht mehr an

Problem: Sentinel zeigt die Change Guardian-Ereignisanlagen nicht an, nachdem Sie die Anlagen einmal angezeigt haben. Die Ereignisanlagen werden nur beim ersten Mal richtig angezeigt. (BUG 902142)

Korrektur: Sentinel 7.3 zeigt die Change Guardian-Ereignisanlagen ordnungsgemäß an.

1.15.10 Unzuverlässige Datenbanksynchronisierung zwischen Sentinel und Sentinel Agent Manager

Problem: In Sentinel Agent Manager (SAM) ausgeführte Aktivitäten wie das Autorisieren eines Agenten werden nicht immer zu Sentinel synchronisiert. Dieses Problem wird durch einen Fehler im ETL-Skript verursacht, das zum Synchronisieren der SAM-Datenbank und der Sentinel-Datenbank verwendet wird. (BUG 885456)

Korrektur: In Sentinel 7.3 wird die Synchronisierung zwischen der SAM-Datenbank und der Sentinel-Datenbank ordnungsgemäß ausgeführt. In SAM ausgeführte Aufgaben werden innerhalb weniger Minuten zu Sentinel synchronisiert.

1.15.11 Ereignisfelder in Bezug auf den geografischen Standort werden nicht mit den richtigen Daten aufgefüllt

Problem: Die Ereignisfelder „Breitengrad“, „Längengrad“ und „Land“ für den Ursprungs-, Ziel- und Observer-Host werden falsch festgelegt.(BUG 895872)

Korrektur: Sentinel füllt die Ereignisfelder „Breitengrad“ und „Längengrad“ nun mit den richtigen Werten auf. Die Ereignisfelder „Land“ werden nun mit dem zweistelligen ISO-Ländercode statt mit dem vollständigen Ländernamen aufgefüllt. Dies bietet eine bessere Kompatibilität mit mehr Gebietsschemen und Visualisierungswerkzeugen.

1.15.12 Skript „clean_db.sh“ löscht die Advisor-Daten in benutzerdefinierten Installationen nicht

Problem: Das Skript `clean_db.sh` löscht Advisor-Daten in benutzerdefinierten Installationen nicht, wenn Advisor-Daten an nicht standardmäßigen Speicherorten vorhanden sind.(BUG 820700)

Korrektur: Das Skript `clean_db.sh` löscht nun die Advisor-Daten an standardmäßigen und benutzerdefinierten Speicherorten.

1.15.13 Verbindungsprobleme zwischen Clients und Sentinel im FIPS-Modus

Problem: Frühere Versionen von Sentinel umfassen Oracle Java 1.7 mit Update 65, bei dem ein bekanntes Problem mit dem Austauschen von RSA-Schlüsseln für Clients im FIPS-Modus vorliegt. Weitere Informationen finden Sie in den Java SE Development Kit 7, Update 51 Release Notes (Versionshinweise für Java SE Development Kit 7, Update 51). Dadurch entstehen Verbindungsprobleme, wenn Sentinel im FIPS-Modus ausgeführt wird und versucht, Verbindungen von Clients wie Security Manager oder Sentinel Agent Manager anzunehmen. (BUG 872305)

Korrektur: Sentinel 7.3 umfasst Oracle Java 1.7 Update 72. Das Problem mit dem Austauschen von RSA-Schlüsseln ist in dieser Version behoben.

1.15.14 Ereignissuche funktioniert nicht nach einer fehlgeschlagenen verteilten Suche

Problem: Wenn bei einer verteilten Suche ein Fehler aufgetreten ist und Sie danach eine Ereignissuche ausführen, gibt Sentinel keine Suchergebnisse zurück. Die Ereignissuche funktioniert nicht mehr und es ist nicht möglich, eine neue Suche auszuführen. (`BUG 864372`)

Korrektur: Sentinel schließt nun die Suchaufträge, die nach einer fehlerhaften Suche warten, und lässt neue Suchen zu.

2 Systemanforderungen

Informationen zu Hardwareanforderungen und unterstützten Betriebssystemen und Browsern finden Sie unter „Meeting System Requirements“ (Erfüllen der Systemanforderungen) im *NetIQ Sentinel Installation and Configuration Guide* (NetIQ Sentinel-Installations- und -Konfigurationshandbuch).

3 Installieren von Sentinel 7.3

Informationen zur Installation von Sentinel 7.3 finden Sie im *NetIQ Sentinel Installation an Configuration Guide* (NetIQ Sentinel-Installations- und -Konfigurationshandbuch).

4 Aufrüsten auf Sentinel 7.3

Sie können von Sentinel 7.0 oder höher auf Sentinel 7.3 aufrüsten.

Laden Sie das Sentinel-Installationsprogramm von der NetIQ-Download-Website herunter. Weitere Informationen zur Aufrüstung auf Sentinel 7.3 finden Sie unter „Upgrading Sentinel“ (Aufrüsten von Sentinel) im *NetIQ Sentinel Installation and Configuration Guide* (NetIQ Sentinel-Installations- und -Konfigurationshandbuch).

4.1 Konfiguration nach der Aufrüstung

Nach der Aufrüstung verfügt die Rolle „Datenvertretungsbenutzer“ nicht über die Berechtigung **Benutzern erlauben, Warnmeldungen zu verwalten**. Die Rolle benötigt diese Berechtigung, um eine Remote-Suche nach Warnmeldungen auszuführen. Weisen Sie der Rolle „Datenvertretungsbenutzer“ die Berechtigung **Benutzern erlauben, Warnmeldungen zu verwalten** manuell zu. Weitere Informationen finden Sie unter „Configuring Roles and Users“ (Konfigurieren von Rollen und Benutzern) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

5 Bekannte Probleme

NetIQ Corporation ist bestrebt, Produkte zu bieten, die hochwertige Lösungen für die Softwarebedürfnisse Ihres Unternehmens darstellen. Die nachfolgend beschriebenen Probleme werden zurzeit untersucht. Wenden Sie sich an den Technischen Support, wenn Sie weitere Hilfe zu einem Problem benötigen.

- Abschnitt 5.1, „SpyEye Tracker-Feeds werden nicht mehr angeboten“, auf Seite 11
- Abschnitt 5.2, „Suche der Tipps-Tabelle gibt in aufgerüsteten Sentinel-Installationen nicht die vollständige Liste der Warnmeldungsfelder zurück“, auf Seite 12
- Abschnitt 5.3, „Sentinel Control Center und Solution Designer können mit JRE 8 nicht gestartet werden, wenn Sentinel im FIPS-Mode ausgeführt wird“, auf Seite 12
- Abschnitt 5.4, „Fehler bei der Datensynchronisierung, wenn IPv6-Adressen im menschenlesbaren Format synchronisiert werden“, auf Seite 12

- Abschnitt 5.5, „Ereignissuche reagiert nicht, wenn Sie über keine Berechtigungen für die Ereignisanzeige verfügen“, auf Seite 13
- Abschnitt 5.6, „Sentinel Agent Manager berücksichtigt die RawDataTapFileSize-Konfiguration nicht“, auf Seite 13
- Abschnitt 5.7, „Beim Bearbeiten einiger gespeicherter Suchen fehlt der Bereich „Ereignisfelder“ auf der Zeitplanseite“, auf Seite 13
- Abschnitt 5.8, „Sentinel gibt keine korrelierten Ereignisse zurück, wenn Sie Ereignisse für die bereitgestellte Regel mit der standardmäßigen Suche über die ausgelöste Anzahl suchen“, auf Seite 13
- Abschnitt 5.9, „Sentinel zeigt im FIPS-Modus keine Informationen zu Change Guardian-Änderungen an“, auf Seite 14
- Abschnitt 5.10, „Geringere Anzahl der Vorkommnisse nach dem Aktualisieren der Warnmeldungsansicht“, auf Seite 14
- Abschnitt 5.11, „Bei der Datenerfassung und Datensynchronisierung mit der DB2-Datenbank tritt nach der Aufrüstung auf Sentinel 7.3 ein Fehler auf“, auf Seite 14
- Abschnitt 5.12, „Neue eingehende Warnmeldungen werden beim Bearbeiten vorhandener Warnmeldungen falsch als ausgewählt angezeigt“, auf Seite 14
- Abschnitt 5.13, „Laden von Sicherheitsintelligenz-Verlaufsdaten dauert lange“, auf Seite 15
- Abschnitt 5.14, „Sicherheitsintelligenz-Dashboard zeigt beim erneuten Generieren einer Grundkonfiguration eine ungültige Grundkonfigurationsdauer an“, auf Seite 15
- Abschnitt 5.15, „Sentinel-Server wird heruntergefahren, wenn eine Suche ausgeführt wird und eine einzelne Partition eine große Anzahl Ereignisse enthält“, auf Seite 15
- Abschnitt 5.16, „Beim Roll-up einer Warnmeldung tritt gelegentlich ein Fehler auf und eine neue Warnmeldung wird erstellt“, auf Seite 15
- Abschnitt 5.17, „Fehler beim Verwenden des Skripts „report_dev_setup.sh“ zum Konfigurieren von Sentinel-Ports für Firewall-Ausnahmen in aufgerüsteten Sentinel-Appliance-Installationen“, auf Seite 16
- Abschnitt 5.18, „Schlechtere Leistung des generischen Sentinel-Collectors, wenn der generische Collector für den Hostnamen-Auflösungsdienst aktiviert wird“, auf Seite 16
- Abschnitt 5.19, „Sentinel kann im FIPS-Modus nicht auf Sicherheitsintelligenzdaten, NetFlow-Daten und Warnmeldungsdaten zugreifen“, auf Seite 16
- Abschnitt 5.20, „Sicherheitsintelligenzdatenbank und Warnmeldungs-Dashboard funktionieren in aufgerüsteten benutzerdefinierten Installationen von Sentinel im FIPS-Modus gelegentlich nicht“, auf Seite 16
- Abschnitt 5.21, „Sentinel zeigt keine Auslöseereignisse für Remote-Warnmeldungen an“, auf Seite 18
- Abschnitt 5.22, „Sentinel zeigt in den Warnmeldungsansichten für Remote-Warnmeldungen keine benutzerdefinierten Warnmeldungseigenschaften an“, auf Seite 18
- Abschnitt 5.23, „Sentinel zeigt nach einem Neustart manchmal keine Warnmeldungen in der Warnmeldungsansicht an“, auf Seite 18
- Abschnitt 5.24, „Fehlende Benutzer in Sicherheitsintelligenzdatenbank in aufgerüsteten Appliance-Installationen“, auf Seite 19
- Abschnitt 5.25, „Sicherheitsschwachstelle in SSL 3.0“, auf Seite 20
- Abschnitt 5.26, „Der Agent Manager-Connector legt die Eigenschaft des Verbindungsmodus in den Ereignissen nicht fest, wenn der verknüpfte Collector mehrere Verbindungsmodi unterstützt“, auf Seite 20

- Abschnitt 5.27, „Sentinel konfiguriert nicht standardmäßig die Netzwerkschnittstelle der Sentinel-Appliance“, auf Seite 20
- Abschnitt 5.28, „Beim Exportieren der Suchergebnisse in Sentinel wird im Webbrowser ein Fehler angezeigt“, auf Seite 21
- Abschnitt 5.29, „Beim Starten der Sentinel-Webkonsole mit Portweiterleitung oder mit Zielnetzwerkadressübersetzung wird eine leere Seite angezeigt“, auf Seite 21
- Abschnitt 5.30, „Beim Erstellen oder Neugenerieren eines Grundwerts wird ein Fehler in Sentinel angezeigt“, auf Seite 21
- Abschnitt 5.31, „Partitionen, die aus dem Sekundärspeicher entfernt werden, werden auch aus dem Primärspeicher entfernt“, auf Seite 21
- Abschnitt 5.32, „Sentinel-Services starten nach der Installation unter Umständen nicht automatisch“, auf Seite 21
- Abschnitt 5.33, „Kerberos-Authentifizierung kann in Sentinel-Appliance-Installationen nicht aktiviert werden“, auf Seite 22
- Abschnitt 5.34, „Remote Collector Manager kann nicht installiert werden, wenn das Passwort Sonderzeichen enthält“, auf Seite 22
- Abschnitt 5.35, „Beim Neustarten eines Remote Collector Manager wird die Verbindung einiger Ereignisquellen unterbrochen“, auf Seite 22
- Abschnitt 5.36, „Die Anzeige von mehreren Berichten gleichzeitig ist nicht möglich“, auf Seite 22
- Abschnitt 5.37, „Bei aktiviertem FIPS-Modus verlangt der Agentenmanager die SQL-Authentifizierung“, auf Seite 22
- Abschnitt 5.38, „Sentinel-Hochverfügbarkeits-Installation im FIPS-Modus gibt einen Fehler zurück“, auf Seite 23
- Abschnitt 5.39, „Sentinel-Hochverfügbarkeits-Installation im Nicht-FIPS-Modus gibt einen Fehler zurück“, auf Seite 23
- Abschnitt 5.40, „Fehler bei der Appliance-Aktualisierung in WebYaST von Versionen vor Sentinel 7.2“, auf Seite 23
- Abschnitt 5.41, „Problem beim Anmelden bei der Sentinel-Appliance“, auf Seite 23
- Abschnitt 5.42, „Fehler beim Installieren von Korrelationsregeln“, auf Seite 24
- Abschnitt 5.43, „Sentinel-Link-Aktion zeigt falsche Meldung an“, auf Seite 24
- Abschnitt 5.44, „Dashboard und Abweichungsdefinitionen mit identischen Namen“, auf Seite 24
- Abschnitt 5.45, „Ungenaue Angaben in den Spalten „Dauer“ und „Zugegriffen“ für aktive Suchaufträge“, auf Seite 24
- Abschnitt 5.46, „Auditereignis „IssueSAMLToken“ zeigt falsche Informationen im Sicherheitsintelligenz-Dashboard an“, auf Seite 24
- Abschnitt 5.47, „Sentinel Control Center wird nicht gestartet, wenn NetIQ Identity Manager Designer auf dem Clientcomputer installiert ist“, auf Seite 25
- Abschnitt 5.48, „Sentinel Agent Manager erfasst keine Windows-Einfügungszeichenketten mit dem Wert „null““, auf Seite 25

5.1 SpyEye Tracker-Feeds werden nicht mehr angeboten

Problem: Der Datenanbieter für SpyEye Tracker-Feeds stellt keine Aktualisierungen mehr für diese Feeds bereit, da SpyEye keine größere Bedrohung mehr darstelle. Das Feed-Plugin ist immer noch im Sentinel-Paket enthalten. Da der Datenanbieter keine gültigen Bedrohungs-Feeds mehr

bereitstellt, füllt das Feed-Plugin die dynamischen Listen mit unerwarteten Daten und verknüpfte Korrelationsregeln arbeiten nicht richtig. Die Benutzeroberfläche der Feeds gibt nur an, dass die Daten erfolgreich verarbeitet wurden, nicht jedoch, dass die Daten ungültig sind. (BUG 916560).

Behelfslösung: Das SpyEye Tracker-Plugin verursacht keine Probleme auf dem Server. Sie können jedoch die Systemressourcen entlasten, indem Sie dieses Feed-Plugin und die verwandten Sentinel-Objekte (dynamische Listen und Korrelationsregeln) entfernen.

Deinstallieren Sie die SpyEye Botnet-Komponente im Lösungspaketemanager. Dadurch werden die verknüpften dynamischen Listen und Korrelationsregeln und das Feed-Plugin entfernt. Wenn das Feed-Plugin jedoch zuvor geplant oder ausgeführt wurde, können Sie es nicht entfernen. In diesem Fall können Sie stattdessen die Aktualisierungen im Zeitplan auf „Nie“ festlegen. Weitere Informationen zum Entfernen der SpyEye Botnet-Komponente im Lösungspaketmanager finden Sie in der Dokumentation zum Threat Intelligence-Lösungspaket auf der Website für Sentinel-Plugins.

5.2 Suche der Tipps-Tabelle gibt in aufgerüsteten Sentinel-Installationen nicht die vollständige Liste der Warnmeldungsfelder zurück

Problem: Wenn Sie in aufgerüsteten Installationen von Sentinel 7.3 in der Tipps-Tabelle in der Webkonsole Warnmeldungsattribute suchen, gibt die Suche nicht die vollständige Liste der Warnmeldungsfelder zurück. Wenn Sie die Suche löschen, werden die Warnmeldungsfelder jedoch richtig in der Tipps-Tabelle angezeigt.(BUG 914755)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

5.3 Sentinel Control Center und Solution Designer können mit JRE 8 nicht gestartet werden, wenn Sentinel im FIPS-Mode ausgeführt wird

Problem: Wenn der Sentinel-Server im FIPS-140-2-Modus ausgeführt wird, können Sentinel Control Center und Solution Designer auf einem Client-Computer mit Java Runtime Environment (JRE) Version 8 oder höher nicht mit Java Web Start gestartet werden. (BUG 910452)

Behelfslösung: Führen Sie auf dem Client-Computer, auf dem Sie Sentinel Control Center oder Solution Designer starten möchten, die folgenden Schritte aus:

- Installieren Sie JRE 7 und verwenden Sie es, um Sentinel Control Center bzw. Solution Designer zu starten.
- Aktivieren Sie im Java Control Panel nicht die Option **TLS 1.2 verwenden** auf der Registerkarte **Erweitert**.

5.4 Fehler bei der Datensynchronisierung, wenn IPv6-Adressen im menschenlesbaren Format synchronisiert werden

Problem: Bei der Datensynchronisierung tritt ein Fehler auf, wenn Sie versuchen, IPv6-Adressfelder im menschenlesbaren Format für externe Datenbanken zu synchronisieren. Informationen über das Konfigurieren von Sentinel zum Auffüllen der IP-Adressfelder in menschenlesbarer Dezimalpunktschreibweise finden Sie unter „Creating a Data Synchronization Policy“ (Erstellen einer Datensynchronisierungsrichtlinie) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch). (BUG 913014)

Behelfslösung: Ändern Sie zur Behebung dieses Problems die maximale Größe der IP-Adressfelder in der Zieldatenbank auf mindestens 46 Zeichen und synchronisieren Sie die Datenbank erneut.

5.5 Ereignissuche reagiert nicht, wenn Sie über keine Berechtigungen für die Ereignisanzeige verfügen

Problem: Wenn Sie eine Ereignissuche ausführen während der Sicherheitsfilter Ihrer Rolle leer ist und die Rolle über keine Berechtigungen zur Ereignisanzeige verfügt, wird die Suche nicht abgeschlossen. Die Suche zeigt keine Fehlermeldung zu den ungültigen Berechtigungen für die Ereignisanzeige an. (BUG 908666)

Behelfslösung: Aktualisieren Sie die Rolle auf eine der folgenden Weisen:

1. Geben Sie im Feld **Nur Ereignisse, die mit diesen Kriterien übereinstimmen** ein Kriterium an. Wenn die Benutzer der Rolle keine Ereignisse sehen sollen, können Sie **NOT sev:[0 TO 5]** eingeben.
2. Wählen Sie **Systemereignisse anzeigen** aus.
3. Wählen Sie **Alle Ereignisdaten anzeigen (einschließlich Rohdaten und NetFlow-Daten)** aus.

5.6 Sentinel Agent Manager berücksichtigt die RawDataTapFileSize-Konfiguration nicht

Problem: Sentinel Agent Manager ignoriert den Wert, der für das Attribut `RawDataTapFileSize` in der Datei `SMServiceHost.exe.config` für die Konfiguration der Rohdatendateigröße angegeben ist, und schreibt nicht mehr in die Rohdatendatei, wenn die Dateigröße 10 MB erreicht.(BUG 867954)

Behelfslösung: Kopieren Sie den Inhalt der Rohdatendatei in eine andere Datei und löschen Sie die Datei, wenn ihre Größe 10 MB erreicht, damit Sentinel Agent Manager erneut Daten in die Datei schreiben kann.

5.7 Beim Bearbeiten einiger gespeicherter Suchen fehlt der Bereich „Ereignisfelder“ auf der Zeitplanseite

Problem: Wenn Sie eine gespeicherte Suche bearbeiten, die von Sentinel 7.2 auf eine spätere Version aufgerüstet wurde, fehlt auf der Zeitplanseite der Bereich **Ereignisfelder**, in dem die Ausgabefelder für die CSV-Datei mit den Suchergebnissen festgelegt werden. (BUG 900293)

Behelfslösung: Erstellen und planen Sie die Suche nach der Aufrüstung von Sentinel neu, damit der Bereich **Ereignisfelder** auf der Zeitplanseite angezeigt wird.

5.8 Sentinel gibt keine korrelierten Ereignisse zurück, wenn Sie Ereignisse für die bereitgestellte Regel mit der standardmäßigen Suche über die ausgelöste Anzahl suchen

Problem: Sentinel gibt keine korrelierten Ereignisse zurück, wenn Sie zum Suchen aller korrelierten Ereignisse, die nach dem Bereitstellen oder Aktivieren der Regel generiert wurden, auf der Korrelationsübersichtsseite der Regel im Bereich **Aktivitätsstatistik** auf das Symbol **Ausgelöste Anzahl** klicken. (BUG 912820)

Behelfslösung: Ändern Sie den Wert im Feld **Von** auf der Seite der Ereignissuche in einen Wert, der einen Zeitpunkt vor der im Feld aufgefüllten Zeit darstellt, und klicken Sie erneut auf **Suchen**.

5.9 Sentinel zeigt im FIPS-Modus keine Informationen zu Change Guardian-Änderungen an

Problem: Sentinel zeigt im FIPS-Modus keine Informationen zu Change Guardian-Änderungen an, wenn Sie Change Guardian-Ereignisse suchen und auf das Symbol **Change Guardian** klicken, auch wenn es zum Empfangen von Change Guardian-Ereignissen konfiguriert ist. Change Guardian 4.1.1.1 und frühere Versionen unterstützen nicht das Senden von Ereignissen im FIPS-kompatiblen Modus.(`BUG 912230`)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

5.10 Geringere Anzahl der Vorkommnisse nach dem Aktualisieren der Warnmeldungsansicht

Problem: Im Feld **Häufigkeit** wird ein kleinerer Wert angezeigt, wenn Sie die Warnmeldungsansicht aktualisieren.(`BUG 913838`)

Behelfslösung: Navigieren Sie zur Seite mit der Warnmeldungszusammenfassung, indem Sie neben der Warnmeldung, für die eine geringerer Wert unter **Häufigkeit** angezeigt wird, auf **Details anzeigen** klicken. Auf der Seite der Warnmeldungszusammenfassung wird im Feld **Häufigkeit** der richtige Wert angezeigt.

5.11 Bei der Datenerfassung und Datensynchronisierung mit der DB2-Datenbank tritt nach der Aufrüstung auf Sentinel 7.3 ein Fehler auf

Problem: Die Aufrüstung auf Sentinel 7.3 verursacht einen Fehler bei der Datenerfassung und Datensynchronisierung mit der DB2-Datenbank, weil der IBM DB2 JDBC-Treiber bei der Aufrüstung entfernt wird.(`BUG 909343`)

Behelfslösung: Fügen Sie nach der Aufrüstung auf Sentinel 7.3 den richtigen JDBC-Treiber hinzu und konfigurieren Sie ihn für die Datenerfassung und Datensynchronisierung. Führen Sie dazu die folgenden Schritte aus:

1. Kopieren Sie die richtige Version des IBM DB2 JDBC-Treibers (`db2jcc-*.jar`) für Ihre DB2-Datenbankversion in den Ordner `/opt/novell/sentinel/lib`.
2. Achten Sie darauf, die erforderliche Eigentümerschaft und die erforderlichen Berechtigungen für die Treiberdatei festzulegen.
3. Konfigurieren Sie diesen Treiber für die Datenerfassung. Weitere Informationen finden Sie in der Datenbank-Connector-Dokumentation.

5.12 Neue eingehende Warnmeldungen werden beim Bearbeiten vorhandener Warnmeldungen falsch als ausgewählt angezeigt

Problem: Wenn Sie in der Warnmeldungsansicht auf **Alle auswählen** klicken, um Warnmeldungen auszuwählen, und dann die Auswahl einiger Warnmeldungen aufheben und diese Warnmeldungen bearbeiten, sind neue eingehende Warnmeldungen in der aktualisierten Warnmeldungsansicht ebenfalls ausgewählt. Dies führt zu einer falschen Anzahl der zur Bearbeitung ausgewählten Warnmeldungen und es könnte angenommen werden, dass neue eingehende Warnmeldungen ebenfalls geändert werden. Es werden jedoch nur die ursprünglich ausgewählten Warnmeldungen bearbeitet.(`BUG 904830`)

Behelfslösung: Wenn Sie die Warnmeldungsansicht mit einem benutzerdefinierten Zeitraum erstellen, werden keine neuen Warnmeldungen in der Warnmeldungsansicht angezeigt.

5.13 Laden von Sicherheitsintelligenz-Verlaufsdaten dauert lange

Problem: Das Laden von Verlaufsdaten der Sicherheitsintelligenz (SI) in Sentinel-Systeme mit hoher EPS-Last dauert lange. (BUG 908599)

Behelfslösung: Wenn Sie ein Sicherheitsintelligenz-Dashboard mit Verlaufsdaten erstellen, planen Sie die Bereitstellung des Dashboards wenn möglich für einen Zeitpunkt mit niedriger Systemlast. Momentan lässt sich dieses Problem nicht anders umgehen.

5.14 Sicherheitsintelligenz-Dashboard zeigt beim erneuten Generieren einer Grundkonfiguration eine ungültige Grundkonfigurationsdauer an

Problem: Während der erneuten Generierung der Sicherheitsintelligenz-Grundkonfiguration werden das Start- und Enddatum falsch als „1.1.1970“ angezeigt.(BUG 912009)

Behelfslösung: Wenn die Neugenerierung der Grundkonfiguration abgeschlossen ist, werden die richtigen Daten angezeigt.

5.15 Sentinel-Server wird heruntergefahren, wenn eine Suche ausgeführt wird und eine einzelne Partition eine große Anzahl Ereignisse enthält

Problem: Der Sentinel-Server wird heruntergefahren, wenn eine Suche ausgeführt wird und eine einzelne Partition eine große Anzahl Ereignisse enthält. (BUG 913599)

Behelfslösung: Erstellen Sie Beibehaltungsrichtlinien so, dass an einem Tag mindestens zwei Partitionen geöffnet sind. Wenn mehrere Partitionen geöffnet sind, wird die Anzahl der in den Partitionen indexierten Ereignisse reduziert.

Sie können Beibehaltungsrichtlinien erstellen, die Ereignisse auf Grundlage des Felds `estzhour` filtern. Dieses Feld dient der Nachverfolgung der Stunde des Tages. Sie können also eine Beibehaltungsrichtlinie mit dem Filter `estzhour:[0 TO 11]` und eine weitere Beibehaltungsrichtlinie mit dem Filter `estzhour:[12 TO 23]` erstellen.

Weitere Informationen finden Sie im Abschnitt „Configuring Data Retention Policies“ (Datenbeibehaltungsrichtlinien konfigurieren) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

5.16 Beim Roll-up einer Warnmeldung tritt gelegentlich ein Fehler auf und eine neue Warnmeldung wird erstellt

Problem: Eine neue Warnmeldung wird erstellt, statt dass die Warnmeldungsinformationen als Roll-up in eine vorhandene Warnmeldung aufgenommen werden. Dieses Problem tritt nur sporadisch auf. (BUG 914512)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

5.17 Fehler beim Verwenden des Skripts „report_dev_setup.sh“ zum Konfigurieren von Sentinel-Ports für Firewall-Ausnahmen in aufgerüsteten Sentinel-Appliance-Installationen

Problem: Sentinel zeigt einen Fehler an, wenn Sie Sentinel-Ports für Firewall-Ausnahmen mit dem Skript `report_dev_setup.sh` konfigurieren. (BUG 914874)

Behelfslösung: Führen Sie die folgenden Schritte aus, um Sentinel-Ports für Firewall-Ausnahmen zu konfigurieren:

1. Öffnen Sie die Datei `/etc/sysconfig/SuSEfirewall2`.
2. Ändern Sie die folgende Zeile:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   in

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Starten Sie Sentinel neu.

5.18 Schlechtere Leistung des generischen Sentinel-Collectors, wenn der generische Collector für den Hostnamen-Auflösungsdienst aktiviert wird

Problem: Die Leistung des generischen Sentinel-Collectors sinkt, wenn der generische Collector für den Hostnamen-Auflösungsdienst unter Microsoft Active Directory und Windows Collector aktiviert wird. Die EPS sinkd um 50 %, wenn Remote-Collector-Manager Ereignisse senden. (BUG 906715)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

5.19 Sentinel kann im FIPS-Modus nicht auf Sicherheitsintelligenzdaten, NetFlow-Daten und Warnmeldungsdaten zugreifen

Problem: Wenn Sie Sentinel im FIPS-Modus installieren, kann der Connector zur Sicherheitsintelligenzdatenbank nicht gestartet werden und Sentinel hat keinen Zugriff auf Sicherheitsintelligenzdaten, NetFlow-Daten und Warnmeldungsdaten. (BUG 915241)

Behelfslösung: Starten Sie Sentinel neu, nachdem Sie es im FIPS-Modus installiert und konfiguriert haben.

5.20 Sicherheitsintelligenzdatenbank und Warnmeldungs-Dashboard funktionieren in aufgerüsteten benutzerdefinierten Installationen von Sentinel im FIPS-Modus gelegentlich nicht

Problem: Wenn Sie von einer benutzerdefinierten Installation von Sentinel, die mit einem Nicht-Root-Benutzer installiert und im FIPS-Modus konfiguriert wurde, auf Sentinel 7.3 aufrüsten, werden die Sicherheitsintelligenzdatenbank und das Warnmeldungs-Dashboard gelegentlich nicht gestartet. (BUG 916285)

Behelfslösung: Führen Sie die folgenden Schritte aus:

1. Wechseln Sie zu <*benutzerdefiniertes Installationsverzeichnis*>/opt/novell/sentinel/bin, um den Sentinel-Indexdienst zu ermitteln.
2. Führen Sie den folgenden Befehl aus:

   ```
   ./si_db.sh status
   ```

   Überprüfen Sie, ob die folgende Ausgabe angezeigt wird:

   ```
   Connection between alert store and indexing service is running.
   Security Intelligence database is running.
   Indexing service is running.
   ```

   Wenn einer der drei oben genannten Dienste nicht ausgeführt wird, führen Sie die folgenden Schritte aus:
3. Führen Sie folgenden Befehl aus, um Sentinel zu stoppen:

   ```
   rcsentinel stop
   ```
4. Melden Sie sich beim Sentinel-Server als der Benutzer „novell“ an.
5. Führen Sie den folgenden Befehl aus:

   <*benutzerdefiniertes Installationsverzeichnis*>/opt/novell/sentinel/bin/si_db.sh startnoauth
6. Führen Sie folgenden Befehl aus, um die Benutzer „dbauser“ und „appuser“ hinzuzufügen:

   ```
   cd <benutzerdefiniertes Installationsverzeichnis>/opt/novell/sentinel/3rdparty/mongodb/bin
   ./mongo
   use admin
   db.addUser ("dbauser", "novell")
   use analytics
   db.addUser ("appuser", "novell")
   exit
   ```
7. Stoppen Sie die MongoDB-Datenbank:

   <*benutzerdefiniertes Installationsverzeichnis*>/opt/novell/sentinel/bin/si_db.sh stop
8. Führen Sie die folgenden Schritte aus, um verschlüsselte Passwortfelder hinzuzufügen:

   8a Führen Sie folgenden Befehl aus, um das verschlüsselte Passwort für den Benutzer „novell“ abzurufen:

   <*benutzerdefiniertes Installationsverzeichnis*>/opt/novell/sentinel/bin/encryptpwd -e novell

   Das verschlüsselte Passwort wird angezeigt. Beispiel:

   ```
   bVWOzu6okMmMCkgM0aHeQ==
   ```

   8b Aktualisieren Sie in der Datei `configuration.properties` die Eigenschaften `baselining.sidb.password` und `baselining.sidb.dbpassword` mit dem verschlüsselten Passwort. Beispiel:

   ```
   baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==
   baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==
   ```

9 Beenden Sie mit dem novell-Benutzerkonto und starten Sie Sentinel mit dem folgenden Befehl mit dem root-Benutzer:

```
rcsentinel start
```

HINWEIS: Führen Sie immer bei Bedarf das Skript `configure.sh` aus, um das Passwort zurückzusetzen. Weitere Informationen zum Ausführen des Skripts `configure.sh` finden Sie unter „Modifying the Configuration after Installation“ (Bearbeiten der Konfiguration nach der Installation) im *NetIQ Sentinel Installation and Configuration Guide* (NetIQ Sentinel-Installations- und -Konfigurationshandbuch).

5.21 Sentinel zeigt keine Auslöseereignisse für Remote-Warnmeldungen an

Problem: Wenn Sie in den Warnmeldungsanischten neben einer Remote-Warnmeldung auf **Details anzeigen** klicken und die Seite mit den Warnmeldungsdetails öffnen, werden die Auslöseereignisse für das betreffende Ereignis im Bereich **Verknüpfte Daten** nicht angezeigt.(`BUG 916116`)

Behelfslösung: Melden Sie sich am Datenquellenserver an und zeigen Sie die Warnmeldungsdetails lokal an.

5.22 Sentinel zeigt in den Warnmeldungsansichten für Remote-Warnmeldungen keine benutzerdefinierten Warnmeldungseigenschaften an

Problem: In den Warnmeldungsansichten werden in den Feldern **Status** und **Priorität** für Remote-Warnmeldungen keine Daten angezeigt, wenn die Werte für diese Felder benutzerdefiniert angepasst wurden. In den Feldern werden auch auf der Seite der Warnmeldungsdetails keine Daten für diese Warnmeldungen angezeigt. (`BUG 915762`)

Behelfslösung: Melden Sie sich am Datenquellenserver an und zeigen Sie die Warnmeldungen lokal an.

5.23 Sentinel zeigt nach einem Neustart manchmal keine Warnmeldungen in der Warnmeldungsansicht an

Problem: Wenn Sie Sentinel neu starten und sich anmelden, zeigt Sentinel manchmal in keiner Warnmeldungsansicht Warnmeldungen an.(`BUG 916133`)

Behelfslösung: Starten Sie die Sicherheitsintelligenzdatenbank neu, indem Sie folgende Schritte ausführen:

1 Führen Sie den folgenden Befehl aus:

```
rm /opt/novell/sentinel/3rdparty/mongoconnector/config.txt
```

2 Bearbeiten Sie `/opt/novell/sentinel/bin/elasticsearch.sh` wie folgt:

2a Geben Sie in der Funktion „es_start()“ wie im folgenden Ausschnitt gezeigt `sleep 2` nach Zeile 209 ein:

```
 exec_command "\"${ESEC_HOME}/3rdparty/elasticsearch/bin/elasticsearch\" -
d -Des.config.file=\"${ESEC_CONFIG_HOME}/3rdparty/elasticsearch/
elasticsearch.yml\" -Des.path.conf=\"${ESEC_CONFIG_HOME}/3rdparty/
elasticsearch\" -Des.path.data=\"${ESEC_DATA_HOME}/3rdparty/elasticsearch/
data\" -Des.path.logs=\"${ESEC_LOG_HOME}/log\""
                if [ $? -ne 0 ]
                then
                        RETRY=$(( $RETRY + 1 ))
                        error_message "$(gettext 'Failed to start indexing
service.')"
                        if [ $RETRY -eq 5 ]
                        then
                        return $RESULT_FAILURE
                        fi
                        sleep 2
                        continue
                fi
                sleep 2
        fi
```

2b Speichern Sie die Datei und beenden Sie den Editor.

3 Führen Sie folgenden Befehl als Benutzer „novell“ aus:

```
/opt/novell/sentinel/bin/si_db.sh restart
```

5.24 Fehlende Benutzer in Sicherheitsintelligenzdatenbank in aufgerüsteten Appliance-Installationen

Problem: In aufgerüsteten Sentinel-Appliance-Online-Installationen sind die Benutzerkonten „appuser“ und „dbauser“ nicht verfügbar. (BUG 915197)

Behelfslösung: Führen Sie die folgenden Schritte aus:

1 Stoppen Sie die Sentinel-Dienste:

```
rcsentinel stop
```

2 Führen Sie den folgenden Befehl aus:

```
/opt/novell/sentinel/bin/si_db.sh startnoauth
```

3 Führen Sie folgenden Befehl aus, um die Benutzer „dbauser“ und „appuser“ hinzuzufügen:

```
cd opt/novell/sentinel/3rdparty/mongodb/bin
./mongo
use admin
db.addUser ("dbauser", "novell")
use analytics
db.addUser ("appuser", "novell")
exit
```

4 Führen Sie den folgenden Befehl aus:

```
/opt/novell/sentinel/bin/si_db.sh stop
```

5 Führen Sie die folgenden Schritte aus, um verschlüsselte Passwortfelder hinzuzufügen:

5a Führen Sie folgenden Befehl aus, um das verschlüsselte Passwort für den Benutzer „novell“ abzurufen:

```
/opt/novell/sentinel/bin/encryptpwd -e novell
```

Das verschlüsselte Passwort wird angezeigt. Beispiel:

```
bVWOzu6okMmMCkgM0aHeQ==
```

5b Aktualisieren Sie in der Datei `configuration.properties` die Eigenschaften `baselining.sidb.password` und `baselining.sidb.dbpassword` mit dem verschlüsselten Passwort. Beispiel:

```
baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==
baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==
```

6 Beenden Sie mit dem novell-Benutzerkonto und starten Sie Sentinel mit dem folgenden Befehl mit dem root-Benutzer:

```
rcsentinel start
```

5.25 Sicherheitsschwachstelle in SSL 3.0

Problem: In SSL 3.0 ist eine Schwachstelle vorhanden, die es unter Umständen ermöglicht, den Text sicherer Verbindungen zu berechnen. Weitere Informationen finden Sie unter CVE-2014-3566. Diese Schwachstelle ist in der gebündelten Version des Syslog-Connector 2011.1r4 vorhanden, da diese das SSL-Protokoll verwendet.

Behelfslösung: Der Syslog-Connector Version 2011.1r5 und höher behebt das Problem. Bis zur offiziellen Freigabe auf der Sentinel-Plugins-Website können Sie den Connector aus dem Bereich Preview (Vorschau) herunterladen.

5.26 Der Agent Manager-Connector legt die Eigenschaft des Verbindungsmodus in den Ereignissen nicht fest, wenn der verknüpfte Collector mehrere Verbindungsmodi unterstützt

Problem: Der Agent Manager-Connector Version 2011.1r3 legt die Eigenschaft CONNECTION_MODE in den Ereignissen nicht fest, wenn der Collector, der die Ereignisse analysiert, mehrere Verbindungsmodi unterstützt. (`BUG 880564`)

Behelfslösung: Der Agent Manager-Connector Version 2011.1r5 und höher behebt das Problem. Bis zur offiziellen Freigabe auf der Sentinel-Plugins-Website können Sie den Connector aus dem Bereich Preview (Vorschau) herunterladen.

5.27 Sentinel konfiguriert nicht standardmäßig die Netzwerkschnittstelle der Sentinel-Appliance

Problem: Die Sentinel-Appliance-Netzwerkschnittstelle ist nicht standardmäßig konfiguriert. (`BUG 867013`)

Behelfslösung: So konfigurieren Sie die Netzwerkschnittstelle:

1. Klicken Sie auf der Seite Netzwerkkonfiguration auf **Network Interfaces** (Netzwerkschnittstellen).
2. Wählen Sie die Netzwerkschnittstelle aus und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Dynamic Address** (Dynamische Adresse) und dann entweder **DHCP** oder **Static assigned IP Address** (Statisch zugewiesene IP-Adresse).
4. Klicken Sie auf **Weiter** und dann auf **OK**.

5.28 Beim Exportieren der Suchergebnisse in Sentinel wird im Webbrowser ein Fehler angezeigt

Problem: Beim Exportieren von Suchergebnissen in Sentinel wird im Webbrowser ggf. ein Fehler angezeigt, wenn Sie die Spracheinstellungen für das Betriebssystem ändern. (BUG 834874)

Behelfslösung: Zum fehlerfreien Exportieren der Suchergebnisse führen Sie einen der folgenden Schritte aus:

- Entfernen Sie beim Exportieren der Suchergebnisse alle Sonderzeichen (außerhalb der ASCII-Zeichen) aus dem Exportdateinamen.
- Aktivieren Sie UTF-8 in den Spracheinstellungen des Betriebssystems, starten Sie den Computer neu und starten Sie dann den Sentinel-Server neu.

5.29 Beim Starten der Sentinel-Webkonsole mit Portweiterleitung oder mit Zielnetzwerkadressübersetzung wird eine leere Seite angezeigt

Problem: Wenn Sie die Sentinel-Webkonsole mit Portweiterleitung oder Zieladressübersetzung (DNAT, Destination Network Address Translation) starten, wird eine leere Seite angezeigt. (BUG 694732)

Behelfslösung: Starten Sie die Sentinel-Webkonsole nicht mit Portweiterleitung oder DNAT (Destination Network Address Translation).

5.30 Beim Erstellen oder Neugenerieren eines Grundwerts wird ein Fehler in Sentinel angezeigt

Problem: Wenn Sie einen Sicherheits-Intelligenzgrundwert erstellen oder neu generieren, so wird der Grundwert ordnungsgemäß erstellt; allerdings wird eine Fehlermeldung angezeigt. (BUG 848067)

Behelfslösung: Diese Meldung können Sie ignorieren. Das Erstellen des Grundwerts kann einige Minuten dauern.

5.31 Partitionen, die aus dem Sekundärspeicher entfernt werden, werden auch aus dem Primärspeicher entfernt

Problem: Wenn der Zeitraum (in Tagen), über den die Daten im Sekundärspeicher verbleiben dürfen, kürzer ist als der Zeitraum (in Tagen) für den Primärspeicher, kann Sentinel den Speicherplatz im Primärspeicher nicht effektiv nutzen. Partitionen, die zum Freigeben von Speicherplatz aus dem Sekundärspeicher entfernt werden, werden auch aus dem Primärspeicher entfernt. (BUG 860888)

Behelfslösung: Ordnen Sie dem Sekundärspeicher ausreichend Speicherplatz zu, damit die Daten über den gesamten vorgesehenen Zeitraum (in Tagen) online und damit suchbar bleiben.

Weitere Informationen finden Sie unter „Event Data (Ereignisdaten)“ im *NetIQ Sentinel Administration Guide (NetIQ-Sentinel-Administrationshandbuch)*.

5.32 Sentinel-Services starten nach der Installation unter Umständen nicht automatisch

Problem: Auf Systemen mit mehr als 2 TB Speicherplatz wird Sentinel nach der Installation unter Umständen nicht automatisch gestartet. (BUG 846296)

Behelfslösung: Starten Sie die Sentinel-Services einmalig manuell, indem Sie den folgenden Befehl eingeben:

```
rcsentinel start
```

5.33 Kerberos-Authentifizierung kann in Sentinel-Appliance-Installationen nicht aktiviert werden

Problem: Wenn Sie in Sentinel-Appliance-Installationen im Kerberos-Modul die Kerberos-Authentifizierung konfigurieren, wird in der Konsole eine Bestätigungsmeldung zur erfolgreichen Konfiguration des Kerberos-Client angezeigt. Wenn Sie das Kerberos-Modul jedoch erneut anzeigen, ist die Option **Kerberos-Authentifizierung aktivieren** nicht ausgewählt. (BUG 843623)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

5.34 Remote Collector Manager kann nicht installiert werden, wenn das Passwort Sonderzeichen enthält

Problem: Wenn Sie bei der Installation eines Remote-Collector-Managers ein Passwort angeben, das Sonderzeichen wie „$“, „"“, „\“ oder „/“ enthält, tritt bei der Installation ein Fehler tritt auf. (BUG 812111)

Behelfslösung: Verwenden Sie keine Sonderzeichen im Passwort für den Remote Collector Manager.

5.35 Beim Neustarten eines Remote Collector Manager wird die Verbindung einiger Ereignisquellen unterbrochen

Problem: Beim Neustarten einer Remote Collector Manager-Appliance wird die Verbindung der Syslog-Ereignisquellen unterbrochen, die mit dem UDP-Port verbunden sind. (BUG 795057)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

5.36 Die Anzeige von mehreren Berichten gleichzeitig ist nicht möglich

Problem: Wenn Sie darauf warten, dass eine PDF-Datei mit Berichtergebnissen angezeigt wird (insbesondere Berichtsergebnisse von 1 Million Ereignissen) und währenddessen auf eine andere PDF-Datei mit Berichtergebnissen klicken, um diese anzuzeigen, dann werden die Berichtergebnisse nicht angezeigt. (BUG 804683)

Behelfslösung: Klicken Sie erneut auf die zweite PDF-Datei mit Berichtergebnissen, um diese anzuzeigen.

5.37 Bei aktiviertem FIPS-Modus verlangt der Agentenmanager die SQL-Authentifizierung

Problem: Wenn der FIPS-Modus in der Sentinel-Umgebung aktiviert ist, führt die Windows-Authentifizierung mit dem Agentenmanager dazu, dass die Synchronisierung mit der Agentenmanager-Datenbank fehlschlägt. (BUG 814452)

Behelfslösung: Verwenden Sie die SQL-Authentifizierung für den Agentenmanager, wenn der FIPS-Modus in der Sentinel-Umgebung aktiviert ist.

5.38 Sentinel-Hochverfügbarkeits-Installation im FIPS-Modus gibt einen Fehler zurück

Problem: Wenn der FIPS-Modus aktiviert ist, wird bei der Sentinel-Hochverfügbarkeitsinstallation der folgende Fehler angezeigt:

```
Die Datei 'configuration.properties' von Sentinel ist falsch. Überprüfen Sie die
Konfigurationsdatei und führen Sie das Skript 'convert_to_fips.sh' erneut aus, um
den FIPS-Modus in Sentinel-Server zu aktivieren.
```

Die Installation wird jedoch erfolgreich abgeschlossen. (BUG 817828)

Behelfslösung: Momentan lässt sich dieses Problem nicht beheben oder umgehen. Die Sentinel-Hochverfügbarkeits-Konfiguration funktioniert problemlos im FIPS-Modus, obwohl das Installationsprogramm den Fehler zurückgibt.

5.39 Sentinel-Hochverfügbarkeits-Installation im Nicht-FIPS-Modus gibt einen Fehler zurück

Problem: Die Sentinel-Hochverfügbarkeitsinstallation im Nicht-FIPS-Modus wird erfolgreich abgeschlossen, es wird jedoch zweimal der folgende Fehler angezeigt:

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: zu viele Argumente
```

(BUG 810764)

Behelfslösung: Momentan lässt sich dieses Problem nicht beheben oder umgehen. Die Sentinel-Hochverfügbarkeits-Konfiguration funktioniert problemlos im Nicht-FIPS-Modus, obwohl das Installationsprogramm den Fehler zurückgibt.

5.40 Fehler bei der Appliance-Aktualisierung in WebYaST von Versionen vor Sentinel 7.2

Problem: Bei Appliance-Aktualisierungen von Versionen vor Sentinel 7.2 tritt ein Fehler auf, weil der Hersteller der Aktualisierungspakete von Novell zu NetIQ geändert wurde. (BUG 780969)

Behelfslösung: Rüsten Sie die Appliance mit dem Befehl "zypper" auf. Weitere Informationen finden Sie unter Upgrading the Appliance by Using zypper (Aufrüsten der Appliance mit zypper) im *NetIQ Sentinel Installation and Configuration Guide* (Installations- und Konfigurationshandbuch für NetIQ Sentinel).

5.41 Problem beim Anmelden bei der Sentinel-Appliance

Problem: Wenn das von Ihnen angegebene Passwort das Zeichen „$“ enthält, speichert Sentinel das Passwort je nach Position des Zeichens „$“ innerhalb des Passworts anders in der Datenbank. Wenn das Passwort mit dem Sonderzeichen „$“ beginnt, speichert Sentinel das Passwort mit einem Dateinamen. Wenn sich das Zeichen „$“ an einer beliebigen Stelle in der Mitte des Passworts befindet, kürzt Sentinel das Passwort bis zur Stelle des Zeichens „$“. (BUG 734500)

Behelfslösung: Das tatsächliche Passwort wird in der Datei `home/novell/.pgpass` gespeichert. Rufen Sie das Passwort aus dieser Datei ab und melden Sie sich dann bei Sentinel an. Wenn Sie beispielsweise „abc$123“ als Passwort angeben, speichert Sentinel das Passwort als „abc“ in der Datei `.pgpass`. Sie können sich bei Sentinel mit dem Passwort „abc“ anmelden.

5.42 Fehler beim Installieren von Korrelationsregeln

Problem: Solution Manager installiert keine Korrelationsregeln, wenn eine Korrelationsregel mit einem identischen Namen bereits im System vorhanden ist. In der Konsole wird der Fehler `NullPointerException` protokolliert. (BUG 713962)

Behelfslösung: Stellen Sie sicher, dass alle Korrelationsregeln einen eindeutigen Namen haben.

5.43 Sentinel-Link-Aktion zeigt falsche Meldung an

Problem: Beim Ausführen einer Sentinel-Link-Aktion über die Sentinel-Webkonsole zeigt Sentinel eine Meldung zum erfolgreichen Abschluss an, obwohl bei der Sentinel-Link-Connector-Integrationsprüfung vom Sentinel Control Center Fehler aufgetreten sind. (BUG 710305)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

5.44 Dashboard und Abweichungsdefinitionen mit identischen Namen

Problem: Wenn ein Sicherheitsintelligenz-Dashboard und eine Abweichungsdefinition identische Namen haben, wird der Dashboard-Link auf der Abweichungsdetailseite deaktiviert. (BUG 715986)

Behelfslösung: Stellen Sie sicher, dass Sie beim Erstellen von Dashboards und Abweichungsdefinitionen eindeutige Namen verwenden.

5.45 Ungenaue Angaben in den Spalten „Dauer“ und „Zugegriffen“ für aktive Suchaufträge

Problem: Die Sentinel-Webkonsole zeigt negative Zahlen in der Spalte mit der Dauer der aktiven Suchaufträge und in der Spalte „Zugegriffen“ an, wenn die Uhrzeit des Sentinel-Webkonsolencomputers hinter der Sentinel-Serveruhrzeit liegt. Beispielsweise zeigen die Spalten „Dauer“ und „Zugegriffen“ negative Zahlen an, wenn die Uhrzeit des Sentinel-Webkonsolencomputers 13:30 Uhr und die des Sentinel-Servers 14:30 Uhr ist. (BUG 719875)

Behelfslösung: Stellen Sie sicher, dass die Uhrzeit auf dem Computer, den Sie zum Zugriff auf die Sentinel-Webkonsole verwenden, der Uhrzeit des Sentinel-Servers entspricht bzw. nach der Uhrzeit des Sentinel-Servers liegt.

5.46 Auditereignis „IssueSAMLToken“ zeigt falsche Informationen im Sicherheitsintelligenz-Dashboard an

Problem: Wenn Sie sich beim Sicherheits-Dashboard anmelden und nach dem `IssueSAMLToken`-Auditereignis suchen, zeigt das `IssueSAMLToken`-Auditereignis einen falschen Hostnamen (InitiatorUserName) oder eine falsche IP-Adresse (SourceIP) an. (BUG 870609)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

5.47 Sentinel Control Center wird nicht gestartet, wenn NetIQ Identity Manager Designer auf dem Clientcomputer installiert ist

Problem: Sentinel Control Center wird nicht gestartet, wenn NetIQ Identity Manager Designer auf dem Clientcomputer installiert ist und das JRE-System verwendet. Designer muss einige unterstützende JAR-Dateien wie `xml-apis.jar` zum Verzeichnis `lib/endorsed` hinzufügen. Einige Klassen in der Datei `xml-apis.jar` überschreiben die entsprechenden Klassen im JRE-System, das von Sentinel Control Center verwendet wird. (`BUG 888085`)

Behelfslösung: Konfigurieren Sie Designer zur Verwendung des eigenen JRE-Systems.

5.48 Sentinel Agent Manager erfasst keine Windows-Einfügungszeichenketten mit dem Wert „null“

Problem: Beim Sammeln von Ereignisdaten erfasst der Sentinel Agent Manager keine Windows-Einfügungszeichenketten, die den Wert „null“ enthalten. (`BUG 838825`)

Behelfslösung: Momentan lässt sich dieses Problem nicht umgehen.

6 Kontaktangaben

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Sie haben Verbesserungsvorschläge? Dann senden Sie sie uns per Email an Documentation-Feedback@netiq.com. Wir freuen uns auf Ihre Rückmeldung.

Ausführliche Kontaktinformationen finden Sie auf der Website mit den Support-Kontaktangaben.

Allgemeine Informationen zu unserem Unternehmen und unseren Produkten finden Sie auf der NetIQ-Firmenwebsite.

Werden Sie Mitglied in unserer Community, und führen Sie interaktive Gespräche mit Fachkollegen und NetIQ-Experten. In der NetIQ-Online-Community finden Sie Produktinformationen, Links zu nützlichen Ressourcen, Blogs und Social-Media-Kanäle.

7 Rechtliche Hinweise

NetIQ Sentinel ist durch folgendes US-Patent geschützt: Nr. 05829001.

DIESES DOKUMENT UND DIE HIER BESCHRIEBENE SOFTWARE WERDEN GEMÄSS EINER LIZENZVEREINBARUNG ODER EINER VERSCHWIEGENHEITSVERPFLICHTUNG BEREITGESTELLT UND UNTERLIEGEN DEN JEWEILIGEN BESTIMMUNGEN DIESER VEREINBARUNGEN. SOFERN NICHT AUSDRÜCKLICH IN DER LIZENZVEREINBARUNG ODER VERSCHWIEGENHEITSVERPFLICHTUNG ERKLÄRT, STELLT DIE NETIQ CORPORATION DIESES DOKUMENT UND DIE IN DIESEM DOKUMENT BESCHRIEBENE SOFTWARE OHNE MÄNGELGEWÄHR UND OHNE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN JEGLICHER ART BEREIT, BEISPIELSWEISE UNTER ANDEREM STILLSCHWEIGENDE GEWÄHRLEISTUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. IN EINIGEN LÄNDERN SIND HAFTUNGSAUSSCHLÜSSE FÜR AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN IN BESTIMMTEN TRANSAKTIONEN NICHT ZULÄSSIG. AUS DIESEM GRUND HAT DIESE BESTIMMUNG FÜR SIE UNTER UMSTÄNDEN KEINE GÜLTIGKEIT.

Der Klarheit halber werden alle Module, Adapter und anderes Material („Modul“) gemäß den Bestimmungen der Endbenutzer-Lizenzvereinbarung (EULA) für die jeweilige Version des NetIQ-Produkts oder der NetIQ-Software lizenziert, zu dem/der diese Module gehören oder mit dem/der sie

zusammenarbeiten. Durch den Zugriff auf ein Modul bzw. durch das Kopieren oder Verwenden eines Moduls erklären Sie sich an diese Bestimmungen gebunden. Falls Sie den Bestimmungen der Endbenutzer-Lizenzvereinbarung nicht zustimmen, sind Sie nicht berechtigt, ein Modul zu verwenden oder zu kopieren bzw. auf ein Modul zuzugreifen, und Sie sind verpflichtet, jegliche Kopien des Moduls zu vernichten und weitere Anweisungen bei NetIQ zu erfragen.

Ohne vorherige schriftliche Genehmigung der NetIQ Corporation dürfen dieses Dokument und die in diesem Dokument beschriebene Software nicht vermietet, verkauft oder verschenkt werden, soweit dies nicht anderweitig gesetzlich gestattet ist. Ohne vorherige schriftliche Genehmigung der NetIQ Corporation darf dieses Dokument oder die in diesem Dokument beschriebene Software weder ganz noch teilweise reproduziert, in einem Abrufsystem gespeichert oder auf jegliche Art oder auf jeglichem Medium (elektronisch, mechanisch oder anderweitig) gespeichert werden, soweit dies nicht ausdrücklich in der Lizenzvereinbarung oder Verschwiegenheitsverpflichtung dargelegt ist. Ein Teil der Unternehmen, Namen und Daten in diesem Dokument dienen lediglich zur Veranschaulichung und stellen keine realen Unternehmen, Personen oder Daten dar.

Dieses Dokument enthält unter Umständen technische Ungenauigkeiten oder Rechtschreibfehler. Die hierin enthaltenen Informationen sind regelmäßigen Änderungen unterworfen. Diese Änderungen werden ggf. in neuen Ausgaben dieses Dokuments eingebunden. Die NetIQ Corporation ist berechtigt, jederzeit Verbesserungen oder Änderungen an der in diesem Dokument beschriebenen Software vorzunehmen.

Einschränkungen für US-amerikanische Regierungsstellen: Wenn die Software und Dokumentation von einer US-amerikanischen Regierungsstelle, im Namen einer solchen oder von einem Auftragnehmer einer US-amerikanischen Regierungsstelle erworben wird, unterliegen die Rechte der Regierung gemäß 48 C.F.R. 227.7202-4 (für Käufe durch das Verteidigungsministerium, Department of Defense (DOD)) bzw. 48 C.F.R. 2.101 und 12.212 (für Käufe einer anderen Regierungsstelle als das DOD) an der Software und Dokumentation in allen Punkten den kommerziellen Lizenzrechten und Einschränkungen der Lizenzvereinbarung. Dies umfasst auch die Rechte der Nutzung, Änderung, Vervielfältigung, Ausführung, Anzeige und Weitergabe der Software oder Dokumentation.

© 2015 NetIQ Corporation. Alle Rechte vorbehalten.

Weitere Informationen zu den Marken von NetIQ finden Sie im Internet unter http://www.netiq.com/company/legal/.